Searching within **The ACM Digital Library** for: content keys for decrypting, setting codes for selection list, property lists (start a new search)

Found **25** of **245,263**

REFINE YOUR SEARCH

Search Results • Related Journals • Related Magazines • Related SIGs • Related Conferences

Refine by Keywords

content keys for decrypt SEARCH

Discovered Terms

Refine by People

Names
Institutions
Authors
Reviewers

Refine by Publications

Publication Year
Publication Names
ACM Publications
All Publications
Content Formats
Publishers

Refine by Conferences

Sponsors
Events
Proceeding Series

ADVANCED SEARCH

Advanced Search

FEEDBACK

Please provide us with feedback

Found **25** of **245,263**

Results 1 - 20 of 25 Sort by relevance in expanded form

Save results to a Binder

Result page: **1** 2 next >>

1 Improved proxy re-encryption schemes with applications to secure distributed storage

Giuseppe Ateniese, Kevin Fu, Matthew Green, Susan Hohenberger

February 2006 **Transactions on Information and System Security (TISSEC)**, Volume 9 Issue 1

Publisher: ACM

Full text available: Pdf (331.59 KB) Additional Information: full citation, abstract, references, index terms, review

Bibliometrics: Downloads (6 Weeks): 40, Downloads (12 Months): 202, Citation Count: 4

In 1998, Blaze, Bleumer, and Strauss (BBS) proposed an application called *atomic proxy re-encryption*, in which a semitrusted proxy converts a ciphertext for Alice into a ciphertext for Bob *without* seeing the underlying plaintext. We predict ...

Keywords: Proxy re-encryption, bilinear maps, double decryption, key translation

2 Pors: proofs of retrievability for large files

Ari Juels, Burton S. Kaliski, Jr.

October 2007 **CCS '07:** Proceedings of the 14th ACM conference on Computer and communications security

Publisher: ACM

Full text available: Pdf (482.87 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 11, Downloads (12 Months): 164, Citation Count: 4

In this paper, we define and explore *proofs of retrievability* (PORs). A POR scheme enables an archive or back-up service (prover) to produce a concise proof that a user (verifier) can retrieve a target file *F*, that is, that the archive ...

Keywords: proofs of knowledge, proofs of retrievability, storage security, storage systems

3 The case for internet voting

Joe Mohen, Julia Glidden

January 2001 **Communications of the ACM** , Volume 44 Issue 1

Publisher: ACM

Full text available: Html (35.34 KB), Pdf (158.11 KB)

Additional Information: full citation, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 33, Downloads (12 Months): 282, Citation Count: 3

4 Gauging the risks of internet elections

Deborah M. Phillips, Hans A. von Spakovsky

January 2001 **Communications of the ACM** , Volume 44 Issue 1

Publisher: ACM

Full text available: Html (35.52 KB), Pdf (159.11 KB)

Additional Information: full citation, references, index terms

Bibliometrics: Downloads (6 Weeks): 19, Downloads (12 Months): 185, Citation Count: 1

5 Design of an UHF RFID transponder for secure authentication

Paolo Bernardi, Filippo Gandino, Bartolomeo Montrucchio, Maurizio Rebaudengo, Erwing Ricardo Sanchez

March 2007 **GLSVLSI '07:** Proceedings of the 17th ACM Great Lakes symposium on VLSI

Publisher: ACM

Full text available: Pdf (347.57 KB)

Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 13, Downloads (12 Months): 163, Citation Count: 0

RFID technology increases rapidly its applicability in new areas of interest without guaranteeing security and privacy issues. This paper presents a new architecture of an RFID transponder with cryptographic capabilities. Other than being compatible ...

Keywords: RFID, authentication, privacy

6 A simple mechanism for capturing and replaying wireless channels

Glenn Judd, Peter Steenkiste

August 2005 **E-WIND '05:** Proceedings of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis

Publisher: ACM

Full text available: Pdf (6.06 MB)

Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 76, Downloads (12 Months): 496, Citation Count: 3

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility ...

Keywords: channel capture, emulation, wireless

7 Communications of the ACM: Volume 51 issue 10

October 2008 Communications of the ACM
Publisher: ACM
Full text available: Digital Edition , Pdf (7.16 MB) Additional Information: full citation

Bibliometrics: Downloads (6 Weeks): 575, Downloads (12 Months): 2432, Citation Count: 0

8 Verifying policy-based web services security

Karthikeyan Bhargavan, Cédric Fournet, Andrew D. Gordon
October 2008 **Transactions on Programming Languages and Systems (TOPLAS)** , Volume 30 Issue 6
Publisher: ACM
Full text available: Pdf (840.56 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 96, Downloads (12 Months): 290, Citation Count: 0

WS-SecurityPolicy is a declarative language for configuring web services security mechanisms. We describe a formal semantics for WS-SecurityPolicy and propose a more abstract language for specifying secure links between web services and their clients. ...

Keywords: Web services, XML security, pi calculus

9 Cryptographically sound implementations for typed information-flow security

Cédric Fournet, Tamara Rezk
January 2008 **POPL '08:** Proceedings of the 35th annual ACM SIGPLAN-SIGACT symposium on Principles of programming languages
Publisher: ACM
Full text available: Pdf (301.13 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 20, Downloads (12 Months): 241, Citation Count: 1

In language-based security, confidentiality and integrity policies conveniently specify the permitted flows of information between different parts of a program with diverse levels of trust. These policies enable a simple treatment of security, and they ...

Keywords: compilers, computational model, confidentiality, cryptography, integrity, non-interference, probabilistic programs, secure information flow, type systems

Also published in:
January 2008 **SIGPLAN Notices** Volume 43 Issue 1

10 Modeling and assessing inference exposure in encrypted databases

Alberto Ceselli, Ernesto Damiani, Sabrina De Capitani Di Vimercati, Sushil Jajodia, Stefano Paraboschi, Pierangela Samarati

February 2005 **Transactions on Information and System Security (TISSEC)** , Volume 8 Issue 1
Publisher: ACM

Full text available: Pdf (727.96 KB) Additional Information: full citation, abstract, references, cited by, index terms

The scope and character of today's computing environments are progressively shifting from traditional, one-on-one client-server interaction to the new cooperative paradigm. It then becomes of primary importance to provide means of protecting the secrecy ...

Keywords: Cryptography, database service, indexing, inference

11 Key management for encrypted broadcast

Avishai Wool

May 2000 **Transactions on Information and System Security (TISSEC)** , Volume 3 Issue 2
Publisher: ACM

Full text available: Pdf (220.36 KB) Additional Information: full citation, abstract, references, index terms

We consider broadcast applications where the transmissions need to be encrypted, such as direct broadcast digital TV networks or Internet multicast. In these applications the number of encrypted TV programs may be very large, but the secure memory capacity ...

Keywords: conditional access, pay-per-view

12 An architecture for secure wide-area service discovery

Todd D. Hodes, Steven E. Czerwinski, Ben Y. Zhao, Anthony D. Joseph, Randy H. Katz

March 2002 **Wireless Networks** , Volume 8 Issue 2/3
Publisher: Kluwer Academic Publishers

Full text available: Pdf (365.68 KB) Additional Information: full citation, abstract, references, cited by, index terms

The widespread deployment of inexpensive communications technology, computational resources in the networking infrastructure, and network-enabled end devices poses an interesting problem for end users: how to locate a particular network service or device ...

Keywords: location services, name lookup, network protocols, service discovery

13 SPINS: security protocols for sensor networks

Adrian Perrig, Robert Szewczyk, J. D. Tygar, Victor Wen, David E. Culler

September 2002 **Wireless Networks** , Volume 8 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: Pdf (213.37 KB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 47, Downloads (12 Months): 256, Citation Count: 77

Wireless sensor networks will be widely deployed in the near future. While much research has focused on making these networks feasible and useful, security has received little attention. We present a suite of security protocols optimized for sensor networks: ...

Keywords: MANET, authentication of wireless communication, cryptography, mobile ad hoc networks, secrecy and confidentiality, secure communication protocols, sensor networks

14 On secure and pseudonymous client-relationships with multiple servers

Eran Gabber, Phillip B. Gibbons, David M. Kristol, Yossi Matias, Alain Mayer

November 1999 **Transactions on Information and System Security (TISSEC)** , Volume 2 Issue 4

Publisher: ACM

Full text available: Pdf (161.56 KB) Additional Information: full citation, abstract, references, cited by, index terms, review

Bibliometrics: Downloads (6 Weeks): 7, Downloads (12 Months): 56, Citation Count: 5

This paper introduces a cryptographic engine, Janus, which assists clients in establishing and maintaining secure and pseudonymous relationships with multiple servers. The setting is such that clients reside on a particular subnet (e. g., corporate intranet, ...

Keywords: Janus function, anonymity, mailbox, persistent relationship, privacy, pseudonym

15 Traps, events, emulation, and enforcement: managing the yin and yang of virtualization-based security

Sergey Bratus, Michael E. Locasto, Ashwin Ramaswamy, Sean W. Smith

October 2008 **VMSec '08:** Proceedings of the 1st ACM workshop on Virtual machine security

Publisher: ACM

Full text available: Pdf (221.17 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 26, Downloads (12 Months): 84, Citation Count: 0

We question current trends that attempt to leverage virtualization techniques to achieve security goals. We suggest that the security role of a virtual machine centers on being a policy interpreter rather than a resource provider. These two roles (security ...

Keywords: debugging, security policy, traps, virtualization

16 An experimental environment for teaching Java security

Anna Riccioni, Enrico Denti, Roberto Laschi

September 2008 **PPPJ '08:** Proceedings of the 6th international symposium on Principles and practice of programming in Java

Publisher: ACM

Full text available: Pdf (641.81 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 21, Downloads (12 Months): 77, Citation Count: 0

In many fields of Computer Engineering education it is crucial that students gain both conceptual understanding and practical skills. To this end, an effective teaching approach relies on a blended-learning strategy that combines face-to-face lessons ...

Keywords: Java cryptography extension, computer engineering education, virtual laboratory

17 A survey on peer-to-peer key management for mobile ad hoc networks

Johann Van Der Merwe, Dawoud Dawoud, Stephen McDonald

April 2007 **Computing Surveys (CSUR)** , Volume 39 Issue 1

Publisher: ACM

Full text available: Pdf (872.71 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 155, Downloads (12 Months): 1334, Citation Count: 6

The article reviews the most popular peer-to-peer key management protocols for mobile ad hoc networks (MANETs). The protocols are subdivided into groups based on their design strategy or main characteristic. The article discusses and provides comments ...

Keywords: Mobile ad hoc networks, pairwise key management, peer-to-peer key management, security

18 Secure attribute-based systems

Matthew Pirretti, Patrick Traynor, Patrick McDaniel, Brent Waters

October 2006 **CCS '06:** Proceedings of the 13th ACM conference on Computer and communications security

Publisher: ACM

Full text available: Pdf (1.13 MB) Additional Information: full citation, abstract, references, cited by, index terms

Bibliometrics: Downloads (6 Weeks): 23, Downloads (12 Months): 208, Citation Count: 6

Attributes define, classify, or annotate the datum to which they are assigned. However, traditional attribute architectures and cryptosystems are ill-equipped to provide security in the face of diverse access requirements and environments. In this paper, ...

Keywords: applied cryptography, attribute-based encryption, secure systems

19 A five-year study of file-system metadata

Nitin Agrawal, William J. Bolosky, John R. Douceur, Jacob R. Lorch

October 2007 **Transactions on Storage (TOS)** , Volume 3 Issue 3

Publisher: ACM

Full text available: Pdf (445.77 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 18, Downloads (12 Months): 243, Citation Count: 1

For five years, we collected annual snapshots of file-system metadata from over 60,000 Windows PC file systems in a large corporation. In this article, we use these snapshots to study temporal changes in file size, file age, file-type frequency, directory ...

Keywords: File systems, generative model, longitudinal study

20 Data Collection with Self-Enforcing Privacy

Philippe Golle, Frank McSherry, Ilya Mironov

December 2008 **Transactions on Information and System Security (TISSEC)** , Volume 12 Issue 2

Publisher: ACM

Full text available: Pdf (315.54 KB) Additional Information: full citation, abstract, references, index terms

Bibliometrics: Downloads (6 Weeks): 94, Downloads (12 Months): 201, Citation Count: 0

Consider a pollster who wishes to collect private, sensitive data from a number of distrustful individuals. How might the pollster convince the respondents that it is trustworthy? Alternately, what mechanism could the respondents insist upon to ensure ...

Keywords: data collection, privacy

Result page: **1** 2 next

>>